Arthur O. Pittenger
Department of Mathematics and Statistics
University of Maryland, Baltimore County
Baltimore, Maryland 21250

Let $H^{(N)}$ denote the tensor product of n finite dimensional Hilbert spaces $H^{(r)}$. A state $|\varphi\rangle$ of $H^{(N)}$ is separable if $|\varphi\rangle = |\alpha_1\rangle \otimes \cdots \otimes |\alpha_n\rangle$ where the states $|\alpha_r\rangle$ are in $H^{(r)}$. An *orthogonal unextendible product basis* is a finite set B of separable orthonormal states $\{|\varphi_k\rangle, 1 \leq k \leq m\}$ such that the non-empty space $B^{\perp}$, the set of vectors orthogonal to B, contains no separable state. Examples of orthogonal UPB sets were first constructed by Bennett et al [1] and other examples and references appear, for example, in [3]. If $F = F(B)$ denotes the set of convex combinations of $\{|\varphi_k\rangle\langle\varphi_k|, 1 \leq k \leq m\}$, then F is a face in the set S of separable densities. In this note we show how to use F to construct families of positive partial transform states (PPT) which are not separable. We also show how to make an analogous construction when the condition of orthogonality is dropped. The analysis is motivated by the geometry of the faces of the separable states and leads to a natural construction of entanglement witnesses separating the inseparable PPT states from S.

I. BACKGROUND

The basic mathematical context of quantum computing and quantum information theory involves a tensor product of Hilbert spaces

$$H^{[N]} = H^{[d_1]} \otimes \ldots \otimes H^{[d_n]},$$

and one of the operational aspects of the theory is the feature of *entanglement* of different factors of the tensor product. The mathematical expression of this feature involves the subset of D, the set of trace one positive semidefinite operators or densities on $H^{[N]}$, which are not in S, the subset of *separable* densities defined as the convex hull of rank one separable projections of the form

$$P = |\varphi\rangle\langle\varphi| = \otimes_{k=1}^{n} |\alpha_k\rangle\langle\alpha_k|.$$

In this notation, P denotes the projection as an operator on $H^{[N]}$, $|\varphi\rangle$ denotes in Dirac notation a normalized non-null eigenvector with $|\varphi\rangle\langle\varphi|$ the Dirac outer product notation for a rank 1 projection, and separability appears in the requirement that $|\varphi\rangle$ is the tensor product of vectors $|\alpha_k\rangle$ in $H^{[d_k]}$. The problem of determining whether a density ρ in the compact, convex set D is also in the smaller compact, convex set S is known as the "separability problem" and has been the subject of much recent research in the quantum computing literature.

All of this abstraction conceals the very real technical problem of constructing in the laboratory a physical entity whose representation is an inseparable density ρ and which has the potential of experimentally realizing some of the rather bizarre predictions of quantum mechanics. In particular, in some circumstances the resulting entanglement between two distinct physical systems can be used as a resource to demonstrate "non-local" behavior between the two systems which may be physically quite far apart. In practice, that means that measurements of the two distinct systems are correlated in ways which cannot be explained by an interpretation based on classical theory.

In 1994 Peter Shor [12] defined an algorithm which could use the quantum mechanical properties of superposition and entanglement to determine the prime factors of a large number M. Since the work factor of the algorithm was polynomial in the number of digits of M, a significant improvement over the best classical factoring algorithms, there was immediate interest in the feasibility of a *quantum computer*, a computing device able to realize quantum mechanical entanglement. As a result, there has been an explosion of theoretical work on the role of quantum mechanics in areas such as computing, cryptography, information theory and complexity theory, and a corresponding growth of experimental work directed at demonstrating some of the theoretical predictions.

In this paper we concentrate exclusively on aspects of the separability problem, and rather than try to summarize all of the relevant references to that subject and to the motivating work mentioned above, we refer the reader to [6] and [11] for references and a development of all aspects of the theory and to [8] which concentrates on the development of quantum computing algorithms and the basics of quantum coding theory. For references to work on the separability problem we recommend the survey paper [13] which gives a good overview of the subject.

II. CONTEXT

Since $H^{[N]}$ is finite dimensional, a density ρ is in S if and only if ρ can be represented as a finite sum

$$\rho = \sum_a p(a) \otimes_{k=1}^n |\alpha_k(a)\rangle \langle \alpha_k(a)|, \tag{1}$$

using the notation above, where $\sum_a p(a) = 1$ with $0 < p(a) \leq 1$. In [7] Peres observed that a necessary condition for ρ to be separable is that its *partial transpositions* are densities. For a general density (with $n = 2$), if one writes ρ as a matrix in a coordinate basis and indexing which respects the tensor product, then the $(i_1 i_2, j_1 j_2)$'th entry of the partial transpose ρ^{T_2} is the $(i_1 j_2, j_1 i_2)$'th entry of ρ. For a separable density one can use complex conjugation and the Hermicity of ρ to write the partial transposition as

$$\rho^{T_2} = \sum_a p(a) |\alpha_1(a)\rangle \langle \alpha_1(a)| \otimes |\alpha_2^*(a)\rangle \langle \alpha_2^*(a)|,$$

and ρ^{T_2} is also a density. In the general case, the superscript will denote partial transposition with respect to a subset of the indices, and the generalized Peres condition is that ρ^T is a density for any such transposition.

As it happens, in the bivariate $2 \otimes 2$ and $2 \otimes 3$ cases the Peres condition is also sufficient: ρ is separable if and only if ρ^{T_2} is a density ([4]). However, for all other cases this is not true: there exist densities which satisfy the Peres condition but which are not in S. Such densities are designated as inseparable PPT (positive partial transform) densities, and it can be shown that physical systems with these densities do not have the kind of entanglement requisite for certain kinds of quantum communication [5]. (See [13] for an exposition and references.)

It is obviously of interest to be able to characterize such PPT densities, and, correspondingly, it is useful to have a way of explicitly constructing examples. An important source of examples is based on the idea of an orthogonal *unextendible product basis* [1]. (Our terminology differs slightly from that in the existing literature by adding orthogonality as a separate property.)

Definition 1 *A set B of separable states*

$$\left\{|\varphi_k\rangle = \otimes_{j=1}^n |\alpha_j(k)\rangle, 1 \leq k \leq m\right\}$$

is an unextendible product basis (UPB) if the non-empty space $B^\perp$, the set of states orthogonal to all of the $|\varphi_k\rangle$, contains no separable state. An orthogonal UPB has the additional constraint that the $|\varphi_k\rangle$'s are orthogonal.

In words, this means that one cannot extend the partial basis B by adding another separable state which is also orthogonal to the states in B. At first glance the construction of such an orthogonal B looks like a difficult problem, but in [1] specific examples are given, and the methodology was extended by DiVincenzo, Terhal and others. (See [13] for references and [1], [3] and [2] for examples.)

The relevance of an orthogonal *UPB* is that it is then easy to construct a specific example of an inseparable density ρ satisfying the Peres condition [14]. Moreover, Terhal also shows that one can use ρ to construct examples of positive but not completely positive operators on $B\left(H^d\right)$, the set of bounded operators on the Hilbert space H^d. We will not go into the definitions and significance of such positive operators here; suffice it to say that they arise in the context of C* algebras and were used in [4] to prove the sufficiency of the Peres condition in the $2 \otimes 2$ case.

One way to analyze the densities in D and S is in the context of the real Hilbert space M which is defined as the set of Hermitian matrices on $H^{[N]}$ with the trace inner product

$$\langle\langle A, B\rangle\rangle = Tr\left(A^\dagger B\right) \tag{2}$$

and Hilbert-Schmidt norm $\|A - B\| = \sqrt{Tr\left((A-B)^2\right)}$. This approach was taken in [9] to get a better perspective of the (Euclidean) geometry of M and the structure of D and S in that context. In fact those tools provide a methodology for finding the nearest separable state to a given inseparable density ρ in particular cases. They also give a way of constructing so-called *entanglement witnesses,* which are simply Hermitian matrices W defining hyperplanes separating an inseparable ρ from S

$$Tr(\rho W) < 0 \leq Tr(\sigma W), all\ \sigma \in S \tag{3}$$

with the hyperplane defined as $\{A \in M : Tr(AW) = 0\}$.

One germane result from [9] is that if τ_0 is the nearest separable state to a non-separable ρ_0, then

$$W_0 \equiv \tau_0 + c_0 I - \rho_0 \tag{4}$$

with $c_0 = Tr\left(\tau_0\left(\rho_0 - \tau_0\right)\right)$ is an entanglement witness for ρ_0 and is related to the Euclidean structure by

$$Tr\left(\sigma W_0\right) = -\left\langle\left\langle\left(\rho_0 - \tau_0\right), \left(\sigma - \tau_0\right)\right\rangle\right\rangle. \tag{5}$$

In particular, the separating hyperplane defined by W_0 contains a face of S:

$$F\left(\tau_0\right) = \left\{\sigma : Tr\left(\sigma W_0\right) = 0, \sigma \in S\right\}.$$

The results in this paper were motivated by combining the techniques and insights in [14] and in [9]. Specifically we examine the geometry implicit in Terhal's construction and use the ideas underlying (4) to define a "geometric" entanglement witness. We then show how to construct a collection of inseparable PPT densities near ρ_0, again motivated by the geometry, and give a sufficient condition for the separating hyperplane defined by ρ_0 to also separate these other PPT densities. Using the resulting insights, we can see the consequences of orthogonality and can give sufficient conditions for comparable constructions when the hypothesis of orthogonality is dropped. In particular, these results provide new perspective on the role of faces of S in the analysis of PPT densities.

III. THE ORTHOGONAL UPB CASE

As above, B denotes an orthogonal unextendible product basis consisting of m separable, orthonormal vectors $|\varphi_k\rangle$, and we define $F\left(B\right) \subset S$ to be the convex hull of the corresponding projections $\mu_k = |\varphi_k\rangle\langle\varphi_k|$:

$$F\left(B\right) = \left\{\mu = \sum_{k=1}^{m} p_k \mu_k, \sum_k p_k = 1\right\}. \tag{6}$$

A key feature of a density in $F\left(B\right)$ is that its convex representation is unique and corresponds to its spectral representation. In fact, $F\left(B\right)$ is a simplex since it is easy to check that each density in $F\left(B\right)$ has a unique convex representation in terms of the μ_k's. Letting D_0 denote the normalized identity $\frac{1}{N}I$, define

$$\mu_0 = \sum \frac{1}{m}\mu_k \text{ and } \rho_0 = \frac{1}{N-m}\left(ND_0 - m\mu_0\right).$$

As a first result, we prove that ρ_0 is an inseparable PPT density, as was shown in [1].

Lemma 1 *ρ_0 is an inseparable PPT density on the boundary of D.*

Proof: From the orthonormality of the $|\varphi_k\rangle$'s,

$$\langle v|\,\rho_0\,|v\rangle = \frac{1}{N-m}\left(\langle v\,|v\rangle - \sum_k \langle v|\,\mu_k\,|v\rangle\right) \geq 0$$

so that ρ_0 is a density. Since each $|\varphi_k\rangle$ is in the null space of ρ_0, ρ_0 is on the boundary of D. (See [9] for the proof that a density is on the boundary of D if and only if it has a non-trivial null space.) Since the $|\varphi_k\rangle$'s are separable projections, it is easy to see that the set $\left\{\mu_k^T, 1 \leq k \leq m\right\}$ of partial transpositions also comes from an unextendible product basis and so each ρ_0^T is also a density. Unwinding the notation as in [14], we see that ρ_0 is proportional to the projector on $B^{\perp}$, and thus its convex representation cannot include separable projections. It follows that ρ_0 is inseparable. (We will give an alternate proof of inseparability below.) □

We next record a key geometric feature of this setup.

Lemma 2 *The "line segment" from μ_0 through D_0 to ρ_0 is orthogonal to $F\left(B\right)$.*

Proof: D_0 is a convex combination of μ_0 and ρ_0, and thus the three are collinear. For each r

$$\left\langle\left\langle\left(D_0 - \mu_0\right), \left(\mu_r - \mu_0\right)\right\rangle\right\rangle = Tr\left(\mu_0^2\right) - Tr\left(\mu_r\mu_0\right) = \frac{1}{m} - \frac{1}{m} = 0,$$

and by linearity the same is true for all σ in $F\left(B\right)$, completing the proof. □

The ideas in the next result come from Terhal's work, and the proof uses the compactness of the set of separable normalized vectors in $H^{[N]}$.

Proposition 1 *inf*$\{Tr\left(\mu_0\sigma\right), \sigma \in S\} \equiv \frac{\epsilon}{m} > 0$ *and the non-empty compact, convex subset of* S

$$G\left(B\right) \equiv \left\{\sigma \in S : Tr\left(\mu_0\sigma\right) = \frac{\epsilon}{m}\right\}$$

is contained in an affine set orthogonal to the line segment from μ_0 *to* ρ_0.

Proof: By convexity, it suffices to take the infimum over the set of separable projections. Suppose that infimum were zero. Then there would be a sequence of separable projections $|\psi_n\rangle$ such that

$$Tr\left(\mu_0 \left|\psi_n\right\rangle \left\langle\psi_n\right|\right) = \frac{1}{m}\sum_k \left|\left\langle\varphi_k\right| \psi_n\right\rangle|^2 \to 0,$$

and by compactness there must be a separable unit vector orthogonal to each of the $|\varphi_k\rangle$. That contradicts the assumption of unextendibility, so the infimum is strictly positive and again by compactness $G\left(B\right)$ must be non-empty. It remains to show the orthogonality. Let σ_1 and σ_2 be trace one Hermitian matrices such that $Tr\left(\mu_0\sigma_k\right) = \frac{\epsilon}{m}$. Then

$$\langle\langle\left(\sigma_1 - \sigma_2\right), \left(\mu_0 - D_0\right)\rangle\rangle = Tr\left(\mu_0\sigma_1\right) - Tr\left(\mu_0\sigma_2\right) = 0,$$

completing the proof. □

There are other geometric aspects of $G\left(B\right)$. For one thing, in some high-dimensional sense $F\left(B\right)$ and $G\left(B\right)$ are parallel since they are perpendicular to the one-dimensional affine space containing ρ_0, D_0, and μ_0. Also, since for any density σ

$$\langle\langle\left(\sigma - D_0\right), \left(\mu_0 - D_0\right)\rangle\rangle = Tr\left(\sigma\mu_0\right) - \frac{1}{N}, \tag{7}$$

we can interpret the inner product to be that between the two "vectors" $\sigma - D_0$ and $\mu_0 - D_0$ in M, and thus $G\left(B\right)$ consists of those separable densities such that

$$\left\|\mu_0 - D_0\right\| \left[\left\|\sigma - D_0\right\| \cos\left(\left(\sigma - D_0\right), \left(\mu_0 - D_0\right)\right)\right] = \frac{\epsilon}{m} - \frac{1}{N}$$

is minimal. Now it is known from a variety of papers, initially in [15] with references and another proof in [10] and [9], that there is a D-neighborhood of the normalized identity D_0 which is composed entirely of separable densities. Hence along the line segment from μ_0 through D_0 to ρ_0, there will be a last separable density $\tilde{\tau}_0$ beyond D_0 and closest to ρ_0. Thus

$$\langle\langle\left(\tilde{\tau}_0 - D_0\right), \left(\mu_0 - D_0\right)\rangle\rangle < 0, \tag{8}$$

implying

$$0 < \frac{N\epsilon}{m} < 1. \tag{9}$$

Putting this all together we see that $G\left(B\right)$ consists of the separable densities σ which, in terms of their projection on the ρ_0 - μ_0 segment, are in the "farthest" face from μ_0.

In defining the entanglement witness in (4), one takes the nearest separable density τ_0 as given and then shows the separating hyperplane contains the analogue of $G\left(B\right)$. In the present context we already know what the separating hyperplane looks like and define the analogue of τ_0. Specifically set $\tau_0\left(s_0\right) = \left(1 - s_0\right) D_0 + s_0\rho_0$, where $0 < s_0 < 1$ is chosen so that $Tr\left(\tau_0\left(s_0\right)\mu_0\right) = \frac{\epsilon}{m}$. Note that we do not claim that $\tau_0\left(s_0\right)$ itself is separable.

Proposition 2 *If* $s_0 = 1 - \frac{\epsilon N}{m}$, $\tau_0 = \tau_0\left(s_0\right)$ *and as usual* $c_0 = Tr\left(\tau_0\left(\rho_0 - \tau_0\right)\right)$, *then* $W_0 = \tau_0 + c_0 I - \rho_0$ *is an entanglement witness for* ρ_0.

Proof: Since $\tau_0\left(s_0\right) = D_0\left(1 + \frac{s_0 m}{N-m}\right) - \frac{s_0 m}{N-m}\mu_0$, one can compute $Tr\left(\tau_0\left(s_0\right)\mu_0\right) = \frac{\epsilon}{m}$ and

$$\frac{1}{N}\left(1 + \frac{s_0 m}{N-m}\right) - \frac{s_0}{N-m} = \frac{\epsilon}{m},$$

giving $s_0 = 1 - \frac{\epsilon N}{m}$. Note that $0 < s_0 < 1$ follows from (9). Since

$$\rho_0 - \tau_0 = \frac{N\epsilon}{N-m}\left(D_0 - \mu_0\right),$$

for separable densities σ

$$\begin{aligned} Tr\left(W_0\sigma\right) &= -Tr\left[\left(\rho_0 - \tau_0\right)\left(\sigma - \tau_0\right)\right] \\ &= \frac{N\epsilon}{N-m}\left[Tr\left(\mu_0\sigma\right) - \frac{\epsilon}{m}\right] \geq 0. \end{aligned} \tag{10}$$

Since $Tr\left(W_0\rho_0\right) < 0$, the proof is complete. □

The preceding proposition confirms what we already knew - that ρ_0 is not separable. In later generalizations we will use this approach to prove inseparability. Before doing that however, let us note that the geometry also suggests a way of constructing other inseparable PPT densities in the vicinity of ρ_0. Pictorially, we work with a given $\mu\left(p\right)$ in $F\left(B\right)$ and "reflect" through D_0 to obtain a corresponding set of $\rho\left(p\right)$'s including ρ_0 on the boundary of D. These $\rho\left(p\right)$'s all have positive partial transforms, and for $\mu\left(p\right)$ in a suitably small neighborhood of μ_0 relative to $F\left(B\right)$ the induced $\rho\left(p\right)$'s are also inseparable.

Keeping the same notation, a density in $F\left(B\right)$ can be written as :

$$\mu\left(p\right) \equiv \sum_k p_k \mu_k \tag{11}$$

where the p_k's are non-negative real numbers with $\sum_k p_k = 1$. Define $b = b\left(p\right) \equiv 1/\max\left(p_k\right) = 1/p_{max}$ and

$$\rho\left(p\right) = \frac{1}{N-b}\left(ND_0 - b\mu\left(p\right)\right). \tag{12}$$

Note that $b \leq m$ with equality if and only if all of the p_k's equal $1/m$.

Proposition 3 *$\rho\left(p\right)$ is a density on the boundary of D. If*

$$p_{max} < \frac{1}{m} + \frac{\epsilon}{m}\left(\frac{N-m}{m-N\epsilon}\right)$$

then $\rho\left(p\right)$ is an inseparable PPT density .

Proof: The proof that $\rho\left(p\right)$ is a density with positive partial transforms is similar to the proof in the first lemma. Since $\rho\left(p\right)$ has a nontrivial null space containing $\left|\varphi_{max}\right\rangle$, it's on the boundary of D. Finally, from (10) $Tr\left(\mu_0\rho\left(p\right)\right) < \frac{\epsilon}{m}$ if and only if p_{max} satisfies the given condition and that gives inseparability. □

We can put all of these results together to obtain a very nice geometric result: inseparable PPT states comprise the entire frustram of the cone with vertex at D_0, "base" defined by the $\rho\left(b\right)$ on the boundary of D and with the other cross-section defined by the separating hyperplane defined by W_0.

Theorem 1 *If $\lambda\left(t\right) = \left(1-t\right)D_0 + t\rho\left(b\right)$, then $\lambda\left(t\right)$ is an inseparable PPT state provided*

$$t\left(b\right) \equiv s_0\left[\frac{Np_{\max} - 1}{N/m - 1}\right] < t \leq 1$$

where $s_0 = 1 - \frac{\epsilon N}{m}$ as above.

Proof: The proof is again simply a matter of checking that $Tr\left(\mu_0\lambda\left(t\right)\right) < \frac{\epsilon}{m}$ when t satisfies the given constraint, and then noticing that $\lambda\left(t\right)$ is a convex combination of PPT states. Note that $t\left(m\right) = s_0$. □

IV. THE NON-ORTHOGONAL CASE

To generalize the theory to the non-orthogonal case, we need to identify some consequences of orthogonality in the preceding analysis. We do that in the subsequent paragraphs, providing an analogous methodology for constructing inseparable densities on the "opposite" side of S from a particular face F. What is lost in this generality, however, is that the resulting inseparable densities are not necessarily PPT. In fact, one can use this "far-face" methodology to represent the maximally entangled state for two qubits $|\psi\rangle\langle\psi|$, where $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, as the ρ_0 obtained from a separable μ_0.

We continue with the notation that B denotes a set of m separable vectors $|\varphi_k\rangle$ but no longer require that they be orthogonal. However, we continue to assume that B is unextendible.

Condition 1: $B^{\perp}$ contains no separable vectors.

One would think that reducing the restrictions on states in B would make it easier to find examples, and that seems to be the case. Rather than working in maximum generality, however, we restrict our attention to $H^{[N]} = H^{[d]} \otimes H^{[d]}$ and record a result found in [1].

Lemma 3 *Let* $B = \{|\varphi_n\rangle = |\alpha_n\rangle \otimes |\beta_n\rangle, 1 \leq n \leq 2d-1\}$ *satisfy the following property:*

$$\begin{array}{l} \textit{every subset of size } d \textit{ of } \{|\alpha_n\rangle, 1 \leq n \leq 2d-1\} \\ \textit{and of } \{|\beta_n\rangle, 1 \leq n \leq 2d-1\} \textit{ is a basis for } H^{[d]} \end{array} \tag{13}$$

Then there is no separable projection $|\varphi\rangle = |\alpha\rangle \otimes |\beta\rangle$ *in* $B^{\perp}$.

Proof: If $\langle\varphi\,|\varphi_n\rangle = 0$, for each n, then there is a subset of indices of size d such that either $\langle\alpha\,|\alpha_n\rangle = 0$ for all such n or $\langle\beta\,|\beta_n\rangle = 0$ for all such n. But any vector orthogonal to a basis is necessarily zero, proving the point. □

Another consequence of the orthogonality assumption is that μ_0 is a density and is in $F(B)$. A weaker condition gives the same result, and we should point out that it may not even be necessary in the analysis to require that μ_0 is actually in $F(B)$.

Condition 2: There exists an m-vector p with non-negative entries such that $\sum_k p_k = 1$ and $\sum_{k=1}^{m} |\langle\varphi_r|\,\varphi_k\rangle|^2 p_k$ is constant.

There are equivalent versions of this condition which may make the motivation clearer. One version is that there is a density

$$\mu_0 = \sum_k p_k \mu_k \tag{14}$$

such that $Tr\left(\mu_0^2\right) = Tr\left(\mu_r \mu_0\right)$ for all r. Another version is that the positive convex cone defined by the columns of the quadratic form $Q(r,k) = Tr\left(\mu_r \mu_k\right) = |\langle\varphi_r|\,\varphi_k\rangle|^2$ contains a constant vector. In the case when the vectors $|\varphi_k\rangle$ are orthogonal, these conditions are easily satisfied, and there is the same geometric interpretation in the non-orthogonal case.

Lemma 4 *Condition 2 is equivalent to the property that the "line segment" from* μ_0 *through* D_0 *is orthogonal to* $F(B)$. □

This condition is also relatively easy to satisfy, and the basic requirement is that the values of $|\langle\varphi_r|\,\varphi_k\rangle|^2$ aren't too large.

Lemma 5 *Suppose that* $\sum_{k\neq r} |\langle\varphi_r|\,\varphi_k\rangle|^2 \leq t < 1$ *for all values of* r. *Then there is a strictly positive probability vector* p *satisfying Condition 2.*

Proof: With $Q(r,k) = |\langle\varphi_r|\,\varphi_k\rangle|^2$, let $B = Q - I$, where I is the identity and thus B is non-negative and zero down the main diagonal. It follows from $\sum_{k=1}^{m} B(r,k) \leq t$ and an induction argument that $\sum_{k=1}^{m} B^{(n)}(r,k) \leq t^n$ for the iterates of B. Let e denote the vector with coordinates equal to 1. Then the equation $Qx = e$ has the solution

$$x = (I+B)^{-1} e = \sum (-1)^k B^k e = \sum B^{2k}(e - Be).$$

Since $e - Be$ is strictly positive, so is x, and $p = x/\sum x_k$ is the desired probability vector. □

Corollary 1 *Under the same hypothesis,* $F(B)$ *is a simplex: each* μ *in* $F(B)$ *has a unique convex representation in terms of the* μ_k*'s.*

Proof: If $\mu = \sum_k p_k \mu_k = \sum_k q_k \mu_k$, then for all j

$$Tr\left(\mu\mu_j\right) = \sum_k Q\left(j,k\right) p_k = \sum_k Q\left(j,k\right) q_k.$$

Since Q is invertible, the assertion is immediate. □

Combining the first two conditions gives the analogue of Proposition 3.1. However, since the spectral representation of μ_0 no longer coincides with its convex representation, we need to introduce explicitly the eigenvalues λ_k of μ_0 with λ_{max} denoting the largest eigenvalue. With exactly the same proof as before, we then have the following result.

Proposition 4 *$inf\{Tr\left(\mu_0\sigma\right), \sigma \in S\} \equiv \epsilon\lambda_{max} > 0$, and the non-empty compact convex subset of S*

$$G\left(B\right) = \{\sigma \in S : Tr\left(\mu_0\sigma\right) = \epsilon\lambda_{max}\}$$

is contained in an affine set orthogonal to the line from μ_0 through D_0. □

Define $b = 1/\lambda_{max}$, so that $b \leq m$, and set

$$\rho_0 = \frac{1}{N-b}\left(ND_0 - b\mu_0\right)$$

as before. Using the spectral representation of μ_0, which is now distinct from its convex representation, familiar arguments confirm the following result. Note that we do not assert that ρ_0 is PPT or even inseparable.

Lemma 6 *ρ_0 is a density on the boundary of D.* □

Conditions 1 and *2* are easily satisfied, but dropping orthogonality introduces a third requirement which is much more restrictive, and this final condition is necessary to complete the extension to the non-orthogonal UPB case. The condition depends heavily on the eigenvalues of μ_0, a fact that is not immediately obvious in the proof of the orthogonal case and which is necessary to obtain the analogue of (9). In the orthogonal case, the right hand side below is zero, and the inequality follows from $\epsilon > 0$.

Condition 3: $\epsilon\lambda_{max} > \left(\lambda_{max} - Tr\left(\mu_0^2\right)\right) / \left(N\lambda_{max} - 1\right)$.

The reasoning behind (8) still applies and this time gives

$$0 < \epsilon N\lambda_{max} < 1, \tag{15}$$

setting the stage for the final bit of analysis.

Theorem 2 *Suppose the set of separable states B satisfies Conditions 1, 2, and 3. Let*

$$s_0 = \frac{\left(1 - \epsilon N\lambda_{max}\right)\left(N\lambda_{max} - 1\right)}{NTr\left(\mu_0^2\right) - 1}.$$

Then $0 < s_0 < 1$. Define $\tau_0 = \tau_0\left(s_0\right) = \left(1 - s_0\right)D_0 + s_0\rho_0$ and use the usual notation to define $W_0 = \tau_0 + c_0 I - \rho_0$. Then τ_0 is a density, and W_0 is an entanglement witness for ρ_0, which is therefore inseparable.

Proof: Each of the factors defining s_0 is positive, so we only need check that $s_0 < 1$. Working out the algebra, which we omit, shows that $s_0 < 1$ is equivalent to *Condition 3*, and thus we know that τ_0 lies strictly between D_0 and ρ_0, although we cannot claim that τ_0 is itself separable. Once we verify that $Tr\left(\mu_0\tau_0\right) = \epsilon\lambda_{max}$, which is a straight-forward calculation, the logic follows the pattern of the analogous result in the orthogonal case, completing the proof. □

I am indebted to the referee for correcting several misstatements in an earlier version of this paper and also for asking for examples illustrating the theory of this section. This led to the results above which show that it is quite easy to give examples of sets B satisfying the first two conditions. In fact, we give an example of a B in the $2 \otimes 2$ case which satisfies *Conditions 1* and *2*, something that is not possible when orthogonality is required ([1]).

Example 1 *Let $d = 2$ and define the three states $|\varphi_n\rangle$, $1 \leq n \leq 3$, by $|\alpha_1\rangle = \frac{1}{\sqrt{2}}1choose1 = |\beta_1\rangle$, $|\alpha_2\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1} = |\beta_2\rangle$, $|\alpha_3\rangle = \frac{1}{\sqrt{2}}\binom{1}{i}$, and $|\beta_3\rangle \frac{1}{\sqrt{2}}\binom{1}{-i}$. Then B_2 satisfies (13), the associated Q matrix is $\begin{pmatrix} 1 & 0 & 1/4 \\ 0 & 1 & 1/4 \\ 1/4 & 1/4 & 1 \end{pmatrix}$, and the p-vector is $(3/8, 3/8, 2/8)$.* □

The real difficulty is with *Condition* 3, and there is no guarantee that a B satisfying the first two conditions will also satisfy the third. In fact one can show that *Condition 3* does not hold in the example above. To illustrate a methodology which simplifies the calculation of λ_{max}, we provide the details.

Lemma 7 *Suppose Conditions 1 and 2 are satisfied and the p-vector is strictly positive. Then the positive eigenvalues of μ_0 coincide with the positive eigenvalues of R where*

$$R(r,n) = p_r \langle \varphi_r | \varphi_n \rangle.$$

Proof: If $\mu_0 |\psi\rangle = \lambda |\psi\rangle$ for positive λ, then necessarily $|\psi\rangle$ is in the span of the $|\varphi_n\rangle$'s: $|\psi\rangle = \sum x_n |\varphi_n\rangle$. Rewriting the eigenvalue equation we obtain

$$\sum_r |\varphi_r\rangle \left[\sum_n R(r,n) x_n - \lambda x_r \right] = 0.$$

Since $Tr(R) = 1$, if R has non-negative eigenvalues, then its positive eigenvalues necessarily coincide with those of μ_0. Using the strict positivity of the components of the probability vector p, $R = D\tilde{R}D^{-1}$ where $\tilde{R}(r,n) = \sqrt{p_r}\langle \varphi_r | \varphi_n \rangle \sqrt{p_n}$ and the diagonal matrix D has entries $\sqrt{p_r}$. But $\tilde{R}$ is a trace one positive semi-definite matrix whose eigenvalues coincide with those of R, and that completes the proof. Note that this approach does not require that the $|\varphi_n\rangle$ be linearly independent. □

Example 2 *In the example from above, one has*

$$R = \begin{pmatrix} 3/8 & 0 & 3/16 \\ 0 & 3/8 & 3/16 \\ 1/8 & 1/8 & 1/4 \end{pmatrix}$$

and computes that μ_0 has positive eigenvalues $\left(5 \pm \sqrt{13}\right)/16$ and $3/8$. The right-hand side of the inequality in Condition 3 equals $\left(5 - \sqrt{13}\right)/16$ and the infimum of $Tr(\mu_0 \sigma)$ appears to be $1/16$, when σ is the density associated with $|\alpha_1\rangle \otimes |\beta_2\rangle$. In any event, Condition 3 does not hold, and the associated ρ_0 is on the same side of the W_0 hyperplane as μ_0. In fact, one can show that ρ_0 is separable. □

To get a positive result, we can perturb examples from the orthogonal case. The idea is to take an orthogonal *UPB* B and slightly modify some of the components of the $|\varphi_n\rangle$'s using a parameter t so that the unextendibility is not lost. If this is done so that $\mu_0(t)$ and its eigenvalues converge to those in the original set B as t goes to 0, then *Condition 3* will be satisfied provided t is small enough:

$$\begin{aligned} Tr(\mu_0(t)\sigma) &= Tr(\mu_0\sigma) + Tr((\mu(t) - \mu_0)\sigma) \\ &\geq \epsilon\lambda_{max} + Tr((\mu(t) - \mu_0)\sigma) \\ &\gtrsim \left(\lambda_{max}(t) - Tr\left(\mu_0^2(t)\right)\right) / (N\lambda_{max}(t) - 1) \to 0. \end{aligned}$$

Example 3 *Take for B the orthogonal "TILES" of the 3×3 case in [1]: $|\varphi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle)$, $|\varphi_2\rangle = \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle)$, $|\varphi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle$, $|\varphi_4\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle$, and $|\varphi_5\rangle = |\gamma\rangle|\gamma\rangle$ where $|\gamma\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$. Modify $|\varphi_5\rangle$ by setting $|\varphi_5\rangle(t) = |\gamma\rangle \frac{1}{\sqrt{c(t)}}((1+t)|0\rangle + |1\rangle + |2\rangle)$ where $c(t)$ is the appropriate normalizing factor. Straightforward computations give*

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & \frac{t^2}{6c(t)} \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \frac{t^2}{6c(t)} & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } p = \frac{1}{5 + \frac{t^2}{2c(t)}} \begin{pmatrix} 1 \\ 1 + \frac{t^2}{6c(t)} \\ 1 + \frac{t^2}{6c(t)} \\ 1 + \frac{t^2}{6c(t)} \\ 1 \end{pmatrix}$$

The eigenvalues are easily computable using the R matrix and are continuous functions of t which converge to $1/5$. Moreover,

$$\left(\lambda_{max}(t) - Tr\left(\mu_0^2(t)\right)\right) / (9\lambda_{max}(t) - 1) = \frac{t}{4\sqrt{6c(t)}} r(t)$$

where $r(t)$ is a rational function converging to 1 as $t \to 0$. Thus, for sufficiently small t, which depends on the value of ϵ, Condition 3 is satisfied.

Acknowledgments: I am indebted to M. Rubin for useful discussions and for pointing out the role of the "far face" of S in the analysis of inseparable densities and to S. Gowda for a delightful discussion which led to the proof of Lemma 4.3. Much of the research for this paper was completed during a visit in the summer of 2001 to the Oxford Centre for Quantum Computation, and the Centre's hospitality is gratefully acknowledged. In independent work, the role of *UPB* bases in constructing *PPT* densities has also been investigated recently by S. Bandyopadhyay, S. Ghosh, and Y. P. Rowchowdhury at UCLA.

---

[1] C. H. Bennett, D. P. DiVincenzo, T. Mor, J. A. Smolin, B. M. Terhal, "Unextendible product bases and bound entanglement", Phys. Rev. Lett. **82**, 5385 (1999).

[2] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal, "Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement", quant-ph/9908070 (Nov. 2000).

[3] D. P. DiVincenzo, B. M. Terhal, "Product Bases in Quantum Information Theory", sub. Proceedings of the XIII International Congress on Mathematical Physics, quant-ph/0008055 (Aug 2000).

[4] M. Horodecki, P. Horodecki, R. Horodecki, "Separability of mixed states: necessary and sufficient conditions", Phys. Lett. A **223**, 1 - 8 (1996).

[5] M. Horodecki, P. Horodecki, R. Horodecki, "Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?", Phys. Rev. Lett. **80**, 5239 (1998).

[6] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press (2000).

[7] A. Peres, "Separability criterion for density matrices", Phys. Rev. Lett. **77**, 1413 (1996).

[8] A. O. Pittenger, *An Introduction to Quantum Computing Algorithms*, Birkhauser Boston, (1999).

[9] A. O. Pittenger, M. H. Rubin, "Convexity and the separability problem of quantum mechanical density matrices", Linear Algebra and its Applications, 346 (1-3) (2002), 47-71 (quant-ph/0103038, (Mar 2001)).

[10] A. O. Pittenger, M. H. Rubin, "Complete separability and Fourier representations of density matrices", Phys. Rev. A **62**, 32313 (2000).

[11] J. Preskill, web site at preskill@theory.caltech.edu.

[12] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", Proc. 37th Symposium on Foundations of Computing, IEEE Computer Society Press, 56 - 65 (1996).

[13] B. M. Terhal, "Detecting quantum entanglement", quant-ph/0101032, (Jan 2001).

[14] B. M. Terhal, "A family of indecomposable positive linear maps based on entangled quantum states", Lin. Alg. Appl. **323**, 61 - 73 (2000).

[15] K. Zyczkowski, P. Horodecki, A. Sanpera, M. Lewenstein, "On the volume of mixed entangled states", Phys. Rev. A **58**, 883 (1998).